1. A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network, the method comprising the steps of

A. with a first set of one or more network elements external to the set of one or more potential victims, diverting to a second set of one or more network elements external to the set of one or more potential victims traffic otherwise destined for the victim,

B. the element(s)of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim.

2. A method according to claim 1, wherein the diverting step includes effecting a path of traffic that differs from a path that traffic would otherwise take to the victim.

3. A method according to claim 1, wherein

the filtering step includes detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differ from expected volume,

the detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly.

4. A method according to claim 1, wherein the filtering step includes detecting suspected malicious traffic.

5. A method according to claim 4, wherein the detecting step includes detecting packets with spoofed source addresses.

6. A method according to claim 5, wherein the filtering step includes detecting traffic requiring a selected service from the victim.

7. A method according to claim 6, wherein the filtering step includes discarding traffic not requiring the selected service from the victim.

8. A method according to claim 7, wherein the filtering step includes discarding any of UDP and ICMP packet traffic.

9. A method according to claim 1, wherein the first set and second set include zero, one or more network elements in common.

10. A method according to claim 1, comprising operating one or more elements of the first set at points on the network around the set of one or more potential victim.

11. A method according to claim 10, comprising operating one or more elements of the second set any of adjacent to or external to one or more elements of the first set.

12. A method according to claim 10, comprising selectively activating one or more elements of the first set to divert traffic to divert traffic to one or more elements of the second set.

13. A method according to claim 12, activating one or more elements of the first sets to divert traffic in response to a distributed denial of service (DDoS) attack, or notification thereof.

14. A method according to claim 12, comprising selectively activating the one or more elements of the first set by any of (i) declaring a network address of the victim to be close in network distance to one or more elements of the second set, and (ii) declaring the network address of the victim to be far from the victim.

15. A method according to claim 12, comprising

associating victim with first and second addresses, and wherein the

filtering step includes

discarding traffic received external to an area defined by the points directed to the first address, and

passing traffic to the victim traffic received external to an area directed to the second address.

16. A method according to claim 10, wherein the diverting step includes redirecting traffic using Policy Based Routing.

17. A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of

A. with a first set of one or more elements external to the set of one or more potential victims, diverting to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim,

B. the element(s)of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim,

C. the filtering step including detecting packets with spoofed source addresses by at least partially processing diverted traffic before selectively passing it, if at all, to the victim.

18. A method according to claim 17, wherein the step of at least partially processing diverted traffic includes executing a verification protocol.

19. A method according to claim 18, wherein the step of at least partially processing diverted traffic includes executing a TCP three-way handshake with a source of diverted traffic.

20. A method according to claim 18, wherein the passing step includes passing to the victim traffic from a source that correctly complies with the handshake protocol.

21. A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of

A. with a first set of one or more elements external to the set of one or more potential victims, diverting to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim,

B. the element(s)of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim,

C. the filtering step including at least partially processing diverted traffic before selectively passing it, if at all, to the victim.

22. A method according to claim 21, wherein the step of at least partially processing diverted traffic includes executing a verification protocol.

23. A method according to claim 22, wherein the step of at least partially processing diverted traffic includes executing a TCP three-way handshake with a source of diverted traffic.

24. A method according to claim 22, wherein the passing step includes passing to the victim traffic from a source that correctly complies with the handshake protocol.

25. A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of

A. with a first set of one or more elements external to the set of one or more potential victims, diverting to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim,

B. the element(s)of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim,

C. the filtering step including discarding traffic of selected type.

26. A method according to claim 25, wherein the filtering step includes discarding any of UDP and ICMP packet traffic.

27. A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of

A. with a first set of one or more elements external to the set of one or more potential victims, performing a first filtering of traffic destined for the victim and diverting to a second set of one or more elements external to the set of one or more potential victims at least a portion of that traffic,

B. the element(s)of the second set performing a second filtering of traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim

28. A method according to claim 27, wherein the first filtering step includes checking an address of traffic against a network interface through which it is received.

29. A method according to claim 28, comprising tracking changes in traffic paths.

30. A method according to claim 29, comprising sampling traffic that arrives on network interfaces.

31. A method according to claim 29, comprising querying apparent sources of traffic to validate legitimacy.

32. A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of

A. with a first set of one or more elements external to the set of one or more potential victims, diverting to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim,

B. the element(s)of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim,

C. the filtering step including identifying any of a source and a type of the overload condition.

33. A method according to claim 32, wherein the identifying step includes statistically measuring any of the traffic pattern and volume.

34. A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of

A. with a first set of one or more elements external to the set of one or more potential victims, diverting to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim,

B. the element(s)of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim,

C. the filtering step including detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differ from expected volume.

35. A method according to claim 34, comprising determining any of a traffic pattern and volume during a period when the victim is not at an overload condition.

36. A method according to claim 35, wherein the determining step includes at least one of

analyzing any of netflow data, server logs, victim traffic, and victim volume, and

classifying any of traffic pattern and volume according to types of users that generated it.

37. A method according to claim 36, wherein the types of users include individuals users, users sharing a host or proxy, web crawlers and monitoring services.

38. A method according to claim 35, wherein the detecting step includes comparing any of a traffic pattern and volume when the victim is at an overload condition with a respective one of a traffic pattern and volume during a period when the victim is not at an overload condition.

39. A method according to claim 38, wherein the comparing step includes determining whether any of the traffic pattern and volume varies statistically with respect to an expected traffic pattern and volume, respectively.

40. A method according to claim 36, wherein the comparing step includes comparing any of traffic volume, port number distribution, periodicity of requests, packet properties, IP geography, and distribution of packet arrival/size.

41. A method according to claim 34, wherein the detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly.

42. A method according to claim 34, wherein the detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly from any of an expected pattern and volume, respectively.

43. A method according to claim 42, comprising determining any of a traffic pattern and volume during a period when the victim is not at an overload condition.

44. A method according to claim 43, wherein the determining step includes analyzing any of netflow data, server logs, victim traffic, and victim volume.

45. A method according to claim 44, wherein any of the determining steps include classifying any of traffic pattern and volume according to types of users that generated it.

46. A network element for use in protecting against an overload condition on a network, the network element comprising:

an input for receiving traffic from the network,

an filter coupled to the input, the filter selectively blocking traffic originating from a source suspected as potentially causing the overload condition,

a statistics module that is coupled to the filter and that identifies traffic statistically indicative of having originated from source potentially causing the overload condition, and

an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter.

47. A network element according to claim 46, comprising a termination detection module that at least participates in determining when the overload condition has ended.

48. A network element according to claim 46, comprising an antispoofing element that any of authenticates and verifies a source of traffic.

49. A system for use in protecting against an overload condition on a network, the network element comprising:

one or more network elements ("guards") disposed on the network, each network element having

an input for receiving traffic from the network,

an filter coupled to the input, the filter selectively blocking traffic originating from a source suspected as potentially causing the overload condition,

a statistics module that is coupled to the filter and that identifies traffic statistically indicative of having originated from a source suspected as potentially causing the overload condition, and

an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter,

one or more further network elements ("diverters") disposed on the network and in communication with the guards, the further network elements selectively (i) diverting to one or more guards traffic otherwise destined for a still further network element ("victim") in a set of one or more potential victims on the network.

50. A system according to claim 49, wherein one or more guards comprises a termination detection module that at least participates in determining when the overload condition has ended.

51. A system according to claim 49, wherein one or more guards comprises an ingress filter, coupled to the statistical module, that generates and transmits to a further network element on the network rules for blocking traffic on the network.

52. A network element according to claim 49, comprising an antispoofing element that any of authenticates and verifies a source of traffic.